

Exhibit B

Summary report:	
Litera Compare for Word 11.3.1.3 Document comparison done on 6/6/2024	
2:07:58 PM	
Style name: Standard	
Intelligent Table Comparison: Active	
Original filename: 36 First Amended Complaint CLEAN.docx	
Modified DMS: iw://qe-us-mobility.imanage.work/QuinnEmanuel/14975866/2	
Changes:	
Add	407
Delete	167
Move From	4
Move To	4
Table Insert	0
Table Delete	2
Table moves to	0
Table moves from	0
Embedded Graphics (Visio, ChemDraw, Images etc.)	0
Embedded Excel	0
Format changes	0
Total Changes:	584

DAVID H. HARPER*

david.harper@haynesboon.com

JASON P. BLOOM*

jason.bloom@haynesboone.com

HAYNES AND BOONE QUINN EMANUEL

URQUHART & SULLIVAN, LLP

Andrew H. Schapiro (*Pro Hac Vice*)

andrewschapiro@quinnemanuel.com

~~2801~~191 N. ~~Harwood Street~~ Wacker Drive,

Suite ~~2300~~2700

Dallas, Texas 75201

Chicago, IL 60606-1881

Telephone: (~~214~~312) ~~651-5000~~705-7400

~~Fa~~simile: (214) 651-5940

David Eiseman (Bar No. 114758)

davideiseman@quinnemanuel.com

50 California Street, 22nd Floor

San Francisco, California 94111-4788

Telephone: 415-875-6600

Fax: 415-875-6700

*~~Admitted~~ Stefan Berthelsen (*Pro Hac Vice*)

JASON T. LAO, SBN 288161

jason.lao@haynesboone.com stefanberthelsen@quinnemanuel.com

51 Madison Ave 22nd floor

New York, NY 10010

ANDREA LEVENSON, SBN 323926

andrea.levenson@haynesboone.com

HAYNES AND BOONE, LLP

600 Anton Boulevard, Suite 700

Costa Mesa, California 92626

Telephone: (~~949~~212) ~~202-3000~~849-7014

~~Fa~~simile: (949) 202-3001

Attorneys for Plaintiff

X Corp.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

X CORP., a Nevada corporation,

Plaintiff,

vs.

BRIGHT DATA LTD., an Israeli
corporation,

Defendant.

Case No. 3:23-cv-03698-WHA

~~FIRST~~SECOND AMENDED
COMPLAINT

JURY TRIAL DEMAND

Plaintiff X Corp. (“X Corp.”, “X”, or “Plaintiff”), by and through its undersigned counsel, hereby files its First Amended Complaint against Defendant Bright Data Ltd., (“Bright Data” or “Defendant”), and in support thereof alleges as follows:

INTRODUCTION

1. Defendant Bright Data Ltd. has built an illicit data-scraping business on the backs of innovative technology companies like X Corp., which operates the social media platform formerly known as Twitter and now known as X. Bright Data scrapes and sells millions of records from X Corp.’s X platform, in blatant violation of X Corp.’s Terms of Service, by which Bright Data is bound. Bright Data also induces and facilitates other X users to violate their own agreements with X Corp. by selling automated data-scraping tools and services that specifically target a wide range of X Corp. data.

2. Bright Data uses elaborate technical measures to evade X Corp.’s anti-scraping technology, taxing the resources of X Corp.’s servers in specific, quantifiable ways and hampering the user experience for legitimate X users.

3. Bright Data is aware that its activities violate X Corp.’s Terms because the company and its executives are registered X account holders who have agreed to abide by those Terms.

4. ~~3-~~ X Corp. brings this action for injunctive relief to halt Bright Data’s unauthorized use of X Corp.’s platform and for damages caused by Bright Data’s breach.

THE PARTIES

5. ~~4-~~ Plaintiff X Corp. is a privately held corporation duly organized and existing under the laws of the State of Nevada with its principal place of business at 1355 Market Street, Suite 900, San Francisco, California, 94103. X Corp. owns and operates the social media platform X, formerly known as Twitter.

6. ~~5-~~ On information and belief, Defendant Bright Data was incorporated in Israel in 2008 as Zon Networks Ltd. and changed its name to Bright Data Ltd. in 2021. Bright Data has its principal place of business at 4 Hamahshev St., Netanya 4250714, in Israel. Bright Data has at times maintained an office at L415 Mission Street, 37th Floor, in San Francisco, California.

7. ~~6.~~ Defendant Bright Data operates brightdata.com, where it sells data scraped from numerous websites and social media platforms, including X, along with tools and services to scrape data from X and other platforms.

JURISDICTION AND VENUE

8. ~~7.~~ This Court has jurisdiction over this action under 28 U.S.C. § 1332 because complete diversity exists, and the amount in controversy exceeds \$75,000. Plaintiff X Corp. is incorporated in Nevada with its principal place of business in California. Defendant Bright Data is incorporated in Israel with its principal place of business in Israel.

9. ~~8.~~ This Court has personal jurisdiction over Defendant because Defendant has consented to X Corp.'s Terms, which require all disputes related to the Terms be brought in the federal or state courts located in San Francisco, California. As part of its agreement to those Terms, Defendant also consented to personal jurisdiction in California.

10. ~~9.~~ Additionally, this Court has personal jurisdiction over Defendant because Defendant knowingly directed prohibited conduct to California and California residents. Defendant offers its data sets and scraping tools for sale in California and to California residents, and has targeted X Corp., which has its principal place of business in California, as well as X Corp.'s users located in California.

11. ~~10.~~ Defendant markets and sells its products to California residents and businesses via a sales office in California, according to its website:

Figure 1: Screenshot of Bright Data's website on November 14, 2023



encouraged customers to contact
page on October 19, 2022

13. ~~12.~~ Members of Defendant’s business development and sales team are also located in California. For example, Defendant’s Chief Revenue Officer, who oversees Bright Data’s sales operations, is based in the San Francisco Bay Area. *See* Exh. C. Defendant’s Global Head of Presales is also based in California, along with numerous other Bright Data employees. *See* Exh. C.

14. ~~13.~~ Defendant has also specifically targeted its products at the California market. For instance, Defendant’s interactive website, through which California residents can purchase Defendant’s scraping tools and scraped data sets, offers a “Superior California Proxy” product that promises “[v]ast numbers of California IPs to get data off any website.”

Figure 3: Screenshot from Bright Data’s website on November 14, 2023



Corp., which has its principal place of business in this district. Defendant also, on information and belief, sold its scraping tools, scraped data sets, and IP Proxies to residents of this district, including through Defendant’s sales office located in this district and employees located in this district.

17. ~~16.~~ Pursuant to Civil L.R. 3-2(d), this case may be assigned to either the San Francisco or Oakland division because X Corp. is located in San Francisco County.

FACTUAL ALLEGATIONS

A. X Corp.'s Platform and Terms of Service

18. ~~17.~~ Plaintiff X Corp. owns and operates the social media platform X, accessible through twitter.com, X.com and various mobile and online applications. X's social media platform is multi-sided with a user side, a developer side, and an advertiser side.

1. The User Side & X. Corp Terms of Service

19. ~~18.~~ The X user platform has hundreds of millions of active users worldwide. More than 23 million X accounts have been registered from California.

20. ~~19.~~ To create a forum for a global conversation about "what's happening," X Corp. allows its registered users to post and share content, including written comments, images and videos, known as posts, and to share, like and comment on other users' posts.

21. ~~20.~~ To post content on X or to re-post, like or otherwise interact with posts by others, users must register for an account and log in to that account.

22. Unlike open access websites, X Corp. does not make its platform and data broadly available to the general public. Rather, in order to gain full access to the X platform when visiting twitter.com, x.com, or downloading the X mobile application, a user must expressly agree to X Corp.'s Terms of Service, Privacy Policy, and the Rules and Policies (collectively the "Terms") by registering for an X account.

23. When an unregistered user visits the X homepage at x.com or twitter.com, the user is invited to create an account or sign in and notified that by signing up, the user will be agreeing to the Terms. Unregistered users are also notified that their unregistered use of the Platform constitutes acceptance of the Terms

24. ~~21.~~ To register for an account, users must provide their name, phone number or email address, and date of birth. To prevent automated services from registering for accounts, X Corp. requires potential account holders to complete a "CAPTCHA" fraud-detection process to determine whether the user is human. CAPTCHA stands for "Completely Automated Public Turing test to tell

1 Computers and Humans Apart.” X Corp. then verifies registrants through email or phone
2 confirmation.

3 25. X users do not pay for basic access to the X user platform, but they can pay for
4 Premium access with extra features.

5 26. ~~22. All~~ Instead, all users who register for a X account, and/or view the X website or
6 application agree to a binding contract with X Corp. as outlined in X Corp.’s User Agreement,
7 which is comprised of the Terms ~~of Service, Privacy Policy, and the Rules and Policies (collectively~~
8 ~~the “Terms”).~~

9 27. ~~23.~~ X Corp.’s Terms state that a user may not “access, tamper with, or use non-public
10 areas of the Services, our computer systems, or the technical delivery systems of our providers” or
11 “breach or circumvent any security or authorization measures.”

12 28. ~~24.~~ X Corp.’s Terms also state a user may not “access or search or attempt to access
13 or search the Services by any means (automated or otherwise) other than through our currently
14 available, published interfaces that are provided by us (and only pursuant to the applicable terms and
15 conditions), unless you have been specifically allowed to do so in a separate agreement with us.”

16 29. ~~25.~~ In addition, X Corp.’s Terms specifically state that “crawling or scraping the
17 Services in any form, for any purpose without our prior written consent is expressly prohibited.”

18 30. ~~26.~~ Under the Terms, users may not “forge any TCP/IP packet header or any part of
19 the header information in any email or posting, or in any way use the Services to send altered,
20 deceptive or false source-identifying information.”

21 31. ~~27.~~ Users are also prohibited under the Terms from any conduct that would “interfere
22 with, or disrupt, (or attempt to do so), the access of any user, host or network, including ...
23 overloading, flooding, spamming ... or by scripting the creation of Content in such a manner as to
24 interfere with or create an undue burden on the Services.”

25 32. ~~28.~~ The Terms also incorporate by reference X Corp.’s Platform Manipulation and
26 Spam Policy (the “Policy”), which specifically prohibits “coordinated harmful activity that
27
28

encourages or promotes behavior which violates [X Corp.’s] Rules.” The Policy also prohibits “leveraging X’s open source code to circumvent remediations or platform defenses.”

33. ~~29.~~ The Terms prohibit selling any content collected from the platform. Users may not “reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly perform, transmit, or otherwise use the Services or Content on the Services” unless otherwise authorized by the Terms or a developer agreement.

~~30. The Terms also expressly state that it is “a violation of these Terms to facilitate or assist others in violating these Terms, including by distributing products or services that enable or encourage violation of these Terms.”~~

~~31. Advertisers on the X platform are also subject to X Corp.’s Ads Policies, which expressly state that advertisers must follow the Terms and all X Corp. Rules.~~

34. The Terms further provide that “[b]y submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods now known or later developed.” This non-exclusive “license authorizes us to make your Content available to the rest of the world and to let others do the same,” but this non-exclusive license is subject to the Privacy Policy.

35. The Privacy Policy allows X users to choose their privacy settings from a menu of privacy options that gives them the ability to withdraw their consent for data sharing, and/or choose what content is publicly shared.

36. X users can adjust their individual privacy settings at any time.

37. X gives users the ability to download their X user data profile which displays what content and information X has collected based on their interactions with the X user platform.

38. X users may also choose to delete their content and/or interactions with posts of other X users.

39. X has platform mechanisms whereby X users subject to the jurisdiction of, for example, the California Consumer Privacy Act or the European Union’s General Data Protection

1 Regulation, may exercise their various privacy rights under those acts, including making certain
 2 deletion requests.

3 *2. The Developer Side & Developer Agreement*

4 40. ~~32.~~ For developers who wish to retrieve or analyze X Corp.'s specialized suite of
 5 select aggregations of user Content into X data, X Corp. offers specialized access to its Application
 6 Programming Interfaces ("APIs") through a tiered subscription service.

7 41. The API subscription service offers developers a Free, Basic, Pro, and Enterprise tier,
 8 each of which offers increasing degrees of access to X data, rate limit relaxations, post-limit
 9 increases, and data analytics from the user side of the X platform.

10 42. To access the Enterprise subscription tier for Twitter's API data access, developers
 11 must affirmatively submit their proposed use cases so that X's developer team can review and
 12 approve.

13 43. IP addresses originating in certain high risk jurisdictions are blacklisted from
 14 accessing X data through the API.

15 44. Not all X user content, including some X user content which is publicly accessible on
 16 the user side of the X platform, however, is packaged in the highest API subscription tier with the
 17 most access to X data. This includes, for example, certain information related to user's specific
 18 geographical locations and other information detailed below.

19 45. Each developer is subject to and bound by X Corp.'s Developer Agreement.

20 46. ~~33.~~ X Corp.'s Developer Agreement also limits the access of developers to X Corp.'s
 21 content. The Agreement instructs developers that they may "not exceed or circumvent rate limits, or
 22 any other limitations or restrictions described in this Policy or your agreement with Twitter, listed on
 23 the Developer Site, or communicated to you by Twitter."

24 47. For the X user content that is available through API access, these restrictions on
 25 developers' utilization of X data through the Developer Agreement include the following.

1 a. X developers must obtain X user consent before sharing specific X user content to
2 promote a product or service, and before storing or sharing non-public or confidential X user
3 information.

4 b. X developers must comply with the protected and blocked status of X content, and
5 API developers are prohibited from circumventing user blocking or account protections.

6 c. X developers must delete from their databases any content that is deleted on X,
7 whether deleted by a user or deleted by X for violations of the Terms or applicable laws—for
8 example, revenge porn content. This includes the eventual deletion—after a maximum of
9 period of 18 months—of all X user content after an X user deactivates or deletes their X
10 account.

11 d. X developers must modify any data modified on X, including when content is made
12 private or deleted.

13 e. X developers must not employ X user geodata on a standalone basis. In other words,
14 X prohibits the development of user tracking, activity heat maps, or similar.

15 f. X developers must not use the X data to create spam, X bot accounts, or automate
16 processes on the X user side such as bulk X user following.

17 g. X developers must not use X data to infer certain protected characteristics of X users
18 which X does not share with developers even if an X user publicly posts this content on X's
19 user platform. These protected characteristics include: health (including pregnancy),
20 negative financial status or condition, political affiliations or belief, racial or ethnic origin,
21 religious or philosophical affiliation or beliefs, sex life or sexual orientation, trade union
22 membership, and whether the user has actually or is alleged to have committed a crime.

23 h. X developers must comply with X user requests which X forwards to them under
24 applicable privacy laws, including the CCPA and GDPR.

25 i. X developers must not attempt to match X content, usernames, or accounts with a
26 person, household, device, browser, or other off-X identifier without the user's express
27

consent, unless the information was provided by the user or is otherwise publicly available (i.e., for public figures).

j. X developers must not use acquired data for tracking or targeting sensitive groups, such as political activists or dissidents, performing background checks or personal vetting, credit or insurance risk analysis, individual profiling or psychographic segmentation, or the development of facial recognition software.

3. The Advertiser Side & Ad Policies

48. Advertisers may purchase targeted ad placements directed towards X users on the X platform subject to X Corp.'s Ads Policies, which expressly state that advertisers must follow the Terms and all X Corp. Rules, including rules in the Developer Agreement.

49. X restricts how advertisers are able to target advertisements to X users based on a variety of protected characteristics.¹

a. X prohibits advertisers from targeting minors with advertisements relating to alcohol, tobacco, firearms, gambling and other inappropriate content.

b. X bans all advertising aimed at minors younger than thirteen.

c. X Corp. requires preapproval for advertising relating to housing, lending, and credit. X generally prohibits advertising targeting user segments sharing sensitive characteristics, including health and pregnancy, negative financial status or condition, political affiliations or belief, race or ethnic origin, religious or philosophical affiliation or beliefs, sex life or sexual orientation, trade union membership, and whether the user has actually or is alleged to have committed a crime—even if X users choose to publicly share this data as content on the X user platform.

¹ Targeting of Sensitive Categories, X Business, <https://business.x.com/en/help/ads-policies/campaign-considerations/targeting-of-sensitive-categories.html> (last visited June 3, 2024).

1 **4. The Balance of X's Multi-Sided Platform Business Model**

2 50. To balance the complex, interrelated nature of its multi-sided platform business and
 3 simultaneously fulfill its use case as a forum for global public conversation on “what’s happening,”
 4 X must be able to credibly enforce its Terms on both its users (both registered and unregistered),
 5 developers, and advertisers. One particular risk is platform and user manipulation of various kinds
 6 through the combined use of both automated aggregated X user data and posting on the X user
 7 platform based on knowledge gleaned from this aggregate data. Policing this problem is made more
 8 difficult when X does not know which entities have gained access to its aggregated X user data
 9 because they have not received it through its tiered subscription service but instead from other
 10 sources, for example, from scraping.

11 51. As part of mitigating these risks, X has a number of Policies which are incorporated
 12 by reference into the Terms and which are intended to prevent nefarious actors from manipulating
 13 users into engaging with accounts or information they otherwise would not.² X regularly disciplines
 14 accounts for breaking this policy, including providing warnings for suspicious content, limiting post
 15 engagement, and account suspension and termination. For example, over a recent six-month period,
 16 X:

- 17 a. Suspended 169,396 accounts and removed 15,275 instances of conduct for violations
 18 of X's policies against sharing improper impersonation;
- 19 b. Suspended 2,563 accounts and removed 62,537 instances of conduct for violations of
 20 X's policies against sharing personally identifiable information; and
- 21 c. Suspended 119,508 accounts and removed 571,902 instances of conduct for
 22 violations of X's policies on illegal and regulated goods.

23 52. X also maintains an active civic integrity policy.³ This policy prohibits false and
 24 misleading information about how to participate in a civic process, including elections, and
 25 established laws relating to civic processes. Users may not post information intended to mislead or

26 ² Platform manipulation and spam policy,
 27 <https://help.x.com/en/rules-and-policies/platform-manipulation>.

28 ³ X Civic integrity policy, <https://help.twitter.com/en/rules-and-policies/election-integrity-policy>.

intimidate voters in order to dissuade them from participating in elections. It also prohibits users from posting account with misleading and deceptive identities. In February 2021, X disclosed it removed 373 accounts and related instances of content attributed to state-linked information operations originating from Iran, Armenia, and Russia. X again disclosed in December 2021 that it removed 3,465 accounts connected to state-linked information operations from eight distinct jurisdictions: Mexico, the People's Republic of China (PRC), Russia, Tanzania, Uganda, and Venezuela. Every account and piece of content associated with these operations was permanently removed from the X platform.

53. X further has policies against both the use of deceptive marketing or misrepresentative business practices,⁴ as well as the advertising of certain high-risk financial products and certain content related to cryptocurrencies.⁵

54. The availability of unrestricted third-party access to scraped data impacts X's ability to accurately and effectively prevent and deter market manipulation, scams, and fraud, increasing the burden on public resources that must be devoted to the regulation and prosecution of such crimes and bad acts, increasing the risk of harm to consumers.⁶

Background on B. Data Scraping & X's Technological Measures Designed to Prevent It

55. ~~34.~~ Scraping is the process of using automated means to collect content or data from a website. The process involves making a request to a website's server, downloading the results and

⁴ *X Deceptive & Fraudulent Content Policy*, <https://business.x.com/en/help/ads-policies/ads-content-policies/deceptive-and-fraudulent-content.html>.

⁵ *X Financial products and services*, <https://business.x.com/en/help/ads-policies/ads-content-policies/financial-services.html>.

⁶ See, e.g., Press Release, SEC, SEC Charges Eight Social Media Influencers in \$100 Million Stock Manipulation Scheme Promoted on Discord and Twitter (Dec. 14, 2022) <https://www.sec.gov/news/press-release/2022-221>; Press Release, U.S. Att'y's Off., N.D. Cal., Scottish Citizen Indicted For Twitter-Based Stock Manipulation Scheme (Nov. 5, 2015), <https://www.justice.gov/usao-ndca/pr/scottish-citizen-indicted-twitter-based-stock-manipulation-scheme>.

1 parsing them to extract the desired data. Data scrapers typically send large volumes of these
2 requests, taxing the capacity of servers and diminishing the experience for legitimate users.

3 56. ~~35.~~ X Corp. utilizes a variety of technological measures to detect and prevent
4 automated systems—colloquially known as bots—from scraping data from its platform, including
5 industry standard automation prevention techniques, such as CAPTCHAs, authorized “guest pass”
6 tokens, registered user identification ~~and~~ limits, IP rate limits, and anomaly detection tools, to put a
7 fence around the X user platform.

8 57. ~~36.~~ X Corp.’s registration process requires potential registrants to pass through the
9 following gates: passing a CAPTCHA; and ~~provide~~ entering a valid phone number or email address.
10 ~~Prior to creating the user’s account, X Corp. sends~~ and inputting a verification code X sent to ~~the~~ that
11 email or phone number. ~~Potential users must enter the verification code to create an account~~ After
12 passing through these technological access gates, X registered users are assigned an X registered
13 user “guest pass” token that grants access to the X platform.

14 58. Although registered users gain access to the X platform and data, guest pass tokens
15 do not grant these users unrestricted access to X’s platform. To protect the X user experience,
16 ensure the functionality of the X platform, and to prevent scraping and automated access, X Corp.
17 limits the access of registered X users in a variety of ways, for example, by setting rate limits on the
18 number of accounts that a registered user may follow in given time periods.

19 59. X employs rate limits as a significant technological measures designed to fence
20 scrapers out of the X user platform because of the massive volume of data available on it:

21 a. On average, about 250 million registered users log in to X every day with 550
22 million unregistered users visiting every month.

23 b. On average, there are about 500 million posts every day.

24 c. Based on internal X investigations, scraping generally entails about a million times
25 more requests to X servers than a normal X user would make.

26 60. Without guest pass tokens, unregistered users’ ability to access X posts or data by
27 visiting x.com, twitter.com, or the X mobile application is highly circumscribed. While

1 unregistered users have never had unfettered access to the X user platform, X has significantly
 2 curtailed this unregistered access in large part to prevent automated user access, including
 3 automated access for the purposes of scraping. Beginning in 2022 and accelerating in the early half
 4 of July 2023, X began to make far less content publicly available for unregistered users as compared
 5 with registered users.

6 61. If an unregistered user now accesses a registered user's profile page, the unregistered
 7 user is shown only a curated sample of the registered user's top posts, rather than all of that user's
 8 posts in chronological order as was previously possible on the X platform. Additionally, an
 9 unregistered user may access a specific, individual post through an external link to that specific post.
 10 Through internet search engines, unregistered users may also access only a limited subset of X
 11 posts—that is, not all posts are available on such search engines and the underlying X post statistics
 12 such as likes, replies, and reposts are no longer available—based on their search results.

13 62. Regardless, unregistered users could never freely browse the X platform or
 14 themselves interact with the posts, but they now cannot access replies to any posts or the user
 15 identities of users who liked those posts.

16 63. These changes have significantly degraded the unregistered X user experience but
 17 were necessary to attempt to tamp automated, unauthorized access to X's platform, including access
 18 by scrapers like Bright Data and its customers.

19 64. In other words, some X user content is designed to be solely accessible to X users,
 20 developers, or advertisers who are logged in to registered X accounts and/or is password-protected,
 21 unless those users circumvent X's technological measures which throttle access.

22 65. Regardless, when viewing the posts to which they have access, unregistered users are
 23 provided with a link to the Terms in the top right corner of the page.

24 66. ~~37. X Corp. also employs rate limits that cap the number of posts that may be viewed~~
 25 ~~by registered users and those who access the platform without an account~~In short, non-registered
 26 users without guest pass tokens have significantly less access to the X user content on the X
 27 platform, and they are subject to significantly higher rate limits. Developers who use the X API are

also capped in the number of posts they may post to, ~~(or pull from)~~ the platform based on their subscription level.

~~38. X Corp. also utilizes anomaly detection to detect and block automated software that is attempting to access X Corp.'s platform.~~

67. For that reason, aggregate data about X content is not publicly available, as casual internet users cannot access it. Accessing aggregate data about X is predicated on agreeing to the various terms and policies. On the other hand, Bright Data offers customers the ability to access “[h]undreds of millions”⁷ of records, some of which may have since been deleted, modified, or made private by X or X users, all without being subject to X’s various restrictions.

C. Catastrophic Damage from Automated Access

68. X employs a microservice server architecture system where its web-hosted applications are run on multiple servers run through two independent data centers. Specific servers within these data centers are allocated to various different software processes within the larger X application ecosystem.

69. In order to account for and avoid the catastrophic failure of X’s platform servers and systems due to this automated circumvention of X rate limits and anomalous bot activity, X obtains an average projected additional 10-20% of over-provisioned headroom for its server load capacity which it would not otherwise purchase in the absence of this circumvention of its technological measures and anomalous bot activity. This additional server load capacity amounts to an average additional cost range of \$10.5 to \$21 million each month for X to run its platform that it would not otherwise incur in the absence of illicit scraping.

70. On average, about 3-5% of total X web traffic is inauthentic and attributable to automated bots or software, including those bots or software employed by Bright Data and marketed to its customers, not human users. On a normal day, X generally receives hundreds of billion unique web requests, so this amounts to tens of billions of daily inauthentic or anomalous web requests

⁷ *Social Media Datasets*, Bright Data, <https://brightdata.com/products/datasets/social-media>.

each day. Specific service path endpoints which are necessary to run X's larger platform but are high risk targets for scraping and demonstrate extremely high proportions of inauthentic and anomalous web requests, including the following:

- a. 99% of web requests to view an individual public user profile are anomalous or inauthentic.
- b. 79% of the web requests to look up a particular user's followers are anomalous or inauthentic.
- c. 80% of the web requests to look up a particular user's followings are anomalous or inauthentic.
- d. 85% of web requests to look up a particular user's tweets and replies are anomalous or inauthentic.
- e. 99% of web requests to access a user's follower graph are anomalous or inauthentic.
- f. 42% of web search query requests of a user's post timeline are anomalous or inauthentic.

71. Because X allocates specific server capacity to specific software service paths, these requests lead to intermittent but individualized internal server failures for the server CPUs hosting these high risk scraping targets. Even when specific servers are overloaded, X's microservice architecture attempts to ensure that the system overall is less likely to fail entirely, but these isolated failures lead to a glitchy, lagged user experience.

72. If X Corp. did not purchase this additional server load capacity and pay the accompanying energy costs, the X user platform would fail at intermittent but regular intervals and thus significantly degrade X's user experience. It is a reputational and business imperative as a public-facing content sharing platform primarily regarding "what's happening" moment to moment that X's servers be available 24/7 with as few outages as possible, so X is forced to incur these additional costs which it would not otherwise bear.

73. On top of server costs, X employs a dedicated team of operational engineers whose job it is to respond and remedy anomalous access on X, which is constantly evolving as X must

understand, assess, and stymie new methods of automated, anomalous, and inauthentic access of its platform. Over the last year, this team responded to and remedied at least 21 major specific instances where scraping was detected. Of course, this team cannot respond to undetected scraping, which Bright Data enables.

74. And outside of the direct costs posed by the data scraping activity, the continued presence of bots, fake profiles, and data scrapers impacts X's relationship with its users, who participate in X's services on a presumption of trust that X can enforce its policies relating to privacy and user content authenticity, among others.

75. Or, if X registered users grow dissatisfied with X's particular cocktail of public-private content-and-data sharing, X users can delete their registered X accounts such that X and its developers eventually delete that content and data as well.

D. Defendant Has Agreed to X Corp.'s Terms of Service

76. ~~39.~~ Defendant has expressly agreed to X Corp.'s Terms and is therefore bound by those Terms.

77. ~~40.~~ Initially, by using the X platform, Defendant, which is well aware of the Terms, agrees to be bound by them. The Terms specifically state:

These Terms of Service ("Terms") govern your access to and use of our services, including our various websites, SMS, APIs, email notifications, applications, buttons, widgets, ads, commerce services, and our other covered services (<https://help.x.com/rules-and-policies/x-services-and-corporate-affiliates>) that link to these Terms (collectively, the "Services"), and any information, text, links, graphics, photos, audio, videos, or other materials or arrangements of materials uploaded, downloaded or appearing on the Services (collectively referred to as "Content"). By using the Services you agree to be bound by these Terms.

78. ~~41.~~ In addition to agreeing to the Terms by using X services, Defendant, which has maintained a registered account on X (@bright_data) since at least February 2016, expressly accepted and agreed to the Terms when registering its account. Bright Data's X account frequently posts content promoting the company's products and services.

79. ~~42.~~ Defendant's top executives are also registered X users and expressly agreed to X Corp.'s Terms when registering their accounts, further demonstrating that Bright Data had knowledge of the Terms:

- a. Bright Data's CEO, Or Lenchner, has maintained a registered account on X (@orlench) since at least December 2012 and regularly posts from that account.
- b. Bright Data's CMO, Yanay Sela, has maintained a registered X account (@yanay_sela) since at least December 2014.
- c. Bright Data's Managing Director for North America, Omri Orgad, has maintained a registered X account (@omri_orgad) since at least November 2011.
- d. Bright Data's Vice President of Product, Erez Naveh, has maintained a registered X account (@nerez) since at least August 2009.
- e. Bright Data's Global Communications Manager, Zachary Keyser, has maintained a registered X account (@KeyserZachary) since at least December 2019.
- f. Bright Data's Founder, Ofer Vilenski, has maintained a registered X account (@vilenski) since at least November 2008.

80. ~~43.~~ On information and belief, several other employees and agents of Defendant involved in Defendant's data-scraping activities are also X account holders, including, by way of example, Artem Shibakov, a Bright Data software engineer who has maintained a registered X account (@ashibakow) since at least February 2013. These account holders have also expressly accepted and agreed to X Corp.'s Terms.

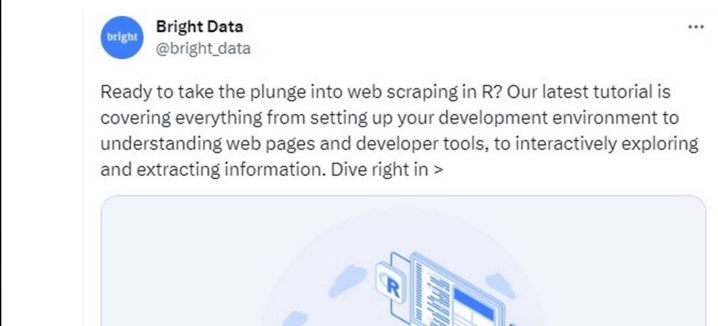
81. ~~44.~~ Defendant is additionally subject to the Terms as an advertiser on X. Beginning on March 7, 2016, Defendant (then known as Luminati Networks) purchased advertising on the X platform. Defendant purchased additional advertising on X from 2019 to 2021. As stated in X Corp.'s Ad Policies, to which Defendant expressly agreed, all advertisers are bound by the platform's Terms and Rules.

82. ~~45.~~ Defendant and its executives have repeatedly used these X accounts to discuss and promote their data-scraping products and services, including but not limited to the following posts:

a. On January 1, 2023, Defendant posted a video on X entitled “How to Scrape UNSCRAPABLE data!” which demonstrated how to use Defendant’s tools and services for unauthorized data scraping.

b. On January 16, 2023, Defendant encouraged users in a post on X to “take the plunge into web scraping” using a “step-by-step guide” to Defendant’s tools and services.

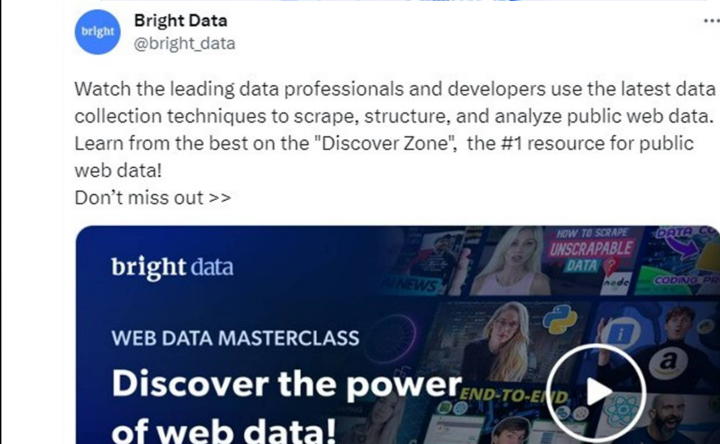
Figure 4: Screenshot of Bright Data’s X post on July 11, 2023



video on X to a “masterclass” that showed scrape, structure, and analyze public web

es.

’s X post on July 11, 2023

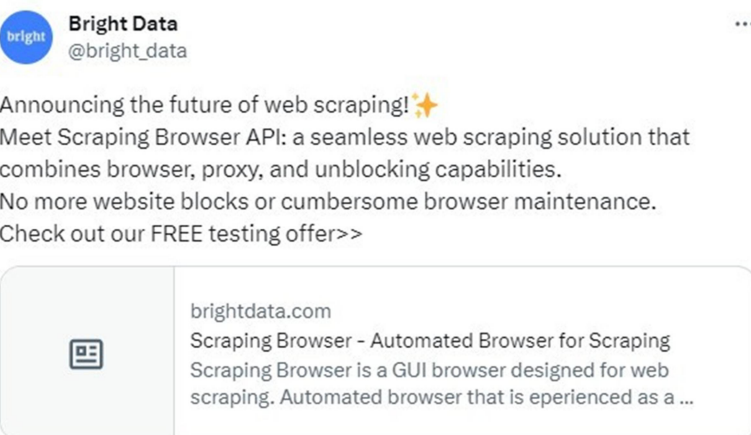


promoted its “Web Unblocker” and its ons” in a post on X.

“Scraping Browser API: a seamless web proxy, and unblocking capabilities” with a

X.

X post on July 11, 2023



engaged in widespread scraping of X violating the Terms to which it agreed. and induced X users to violate X Corp.’s

84. 47. X Corp. has not granted Defendant permission to scrape data from the X platform.

85. 48. X Corp permits paying ~~customers~~ developers and advertisers to lawfully access certain categories of X data, subject to contractual usage limits and other restrictions designed to protect the X platform and user experience as detailed above. Rather than attempt to lawfully acquire X data through authorized means, Bright Data elected to scrape the data (and enable others to do so), using proxies and other illicit methods to shield its identity and scraping activities.

86. 49. Defendant has not publicly disclosed how it evades X Corp.'s technical safeguards against scraping. However, Defendant's website makes clear that the company engages in prohibited scraping on an industrial scale and brazenly advertises that Defendant sells tools and services that encourage and enable others to engage in prohibited scraping.

87. Defendant's public reputation is that it is a market leader in scraping social media platforms such as X on a massive scale.

Defendant Scrapes and Sells X Corp. Data

88. 50. As seen in Figure 7 below, Defendant offers X Corp.'s data for sale on its website.

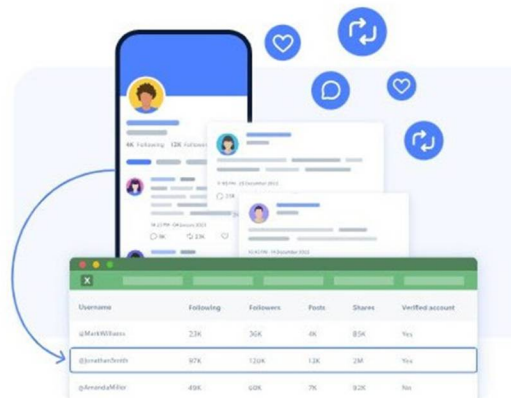
Figure 7: Screenshot of Bright Data's website on July 10, 2023

DATASETS

Twitter Datasets

Tap into Twitter public accounts with Bright Data's Twitter dataset. Use innovative filtering capabilities to monitor sentiment, identify trends, or locate the right influencers, it's really up to you.

[Request dataset >](#)



a sets offered for sale by .” Specifically, these data
ount type, links, bio, brand
re.”
/ 10, 2023

Twitter Datasets

Added and enriched data points on top of the data extracted from Twitter may include:
of followers, verified, account type, links, bio, brand affiliation, posts, images, tweets, shares, location, hashtags, and much more.

Timestamp	ID	URL	Image URL
2023-02-15	ODN24011N9	https://www.example.com/5TE345...	https://www.image.com/img_F4TTVC
2023-02-14	29F9H294HDN	https://www.example.com/5F4556...	https://www.image.com/img_35TGRO2
2023-02-14	IEFN3816F3B94	https://www.example.com/435F56Y...	https://www.image.com/img_G29JFVG
2023-02-13	3P9HQ491YK5	https://www.example.com/7HBT394...	https://www.image.com/img_7DNH9AS
2023-02-11	HE13H589H0J2	https://www.example.com/96E1397...	https://www.image.com/img_849483
2023-02-11	RTQ452P54H4	https://www.example.com/V438VY5...	https://www.image.com/img_53E345V

BRIGHT DATA LTD.

1 90. ~~52.~~ Defendant could have only obtained this data by engaging in prohibited scraping
2 of X's platform.

3 91. ~~53.~~ Defendant offers this unlawfully obtained data for sale starting at \$.01 per record,
4 but also offers customized packages of X Corp.'s data.

5 92. ~~54.~~ Defendant also offers several options for delivery of X Corp.'s data, and even
6 offers its customers the opportunity to regularly update its data sets with additional data scraped
7 from X at regular intervals.

8 ***Bright Data Sells Automated Tools to Scrape X Corp.'s Data***

9 93. ~~55.~~ Defendant also offers for sale on its website automation software that allows
10 users to scrape data directly from the X platform in violation of X Corp.'s Terms.

11 94. ~~56.~~ As indicated in Exhibit F, Defendant's website states: "If you don't want to
12 purchase a Twitter dataset, you can start scraping Twitter public data using our Web Scraper IDE."

13 **Figure 9: Screenshot of Bright Data's website on July 10, 2023**

Can I scrape Twitter's public data by myself?

If you don't want to purchase a Twitter dataset, you can start scraping Twitter public data using our [Web Scraper IDE](#).

to evade detection utilizing a
ss geo-restricted content, and

18 improve scraping speed." The tool also includes an "unblocking solution" that is designed to evade
19 anti-scraping measures like those employed by X Corp. Defendant specifically advertises that its
20 Web Scraper tool can be used to "[e]asily scrape data from any geo-location while avoiding
21 CAPTCHAs and blocks."

22 96. ~~58.~~ In addition to its Web Scraper tool, Defendant sells at least four additional tools
23 designed to scrape information specifically from the X Platform: Twitter Scraper, Twitter Profile
24 Scraper, Twitter Image Scraper, and Twitter Followers Scraper.

- 25 a. As seen in Figure 7 below, Defendant offers a Twitter Scraper to automatically
26 scrape data from the X platform, including "URLs, hashtags, images, videos, tweets,
27 retweets, conversation threads, followers/following, locations, and more."

Figure 10: Screenshot of Bright Data's website on July 10, 2023

1

Twitter Scraper

Scrape Twitter and scrape data such from public Twitter profiles. Collect data on URLs, hashtags, images, videos, tweets, retweets, conversation threads, followers/following, locations, and more.

[Start Free Trial >](#)



Twitter Profile Scraper to
name, likes, tweets and
followers, URL, date of

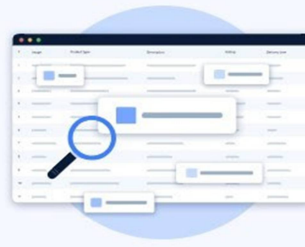
10, 2023

8 ||

Twitter Profile Scraper

Scrape Twitter profiles (public) and collect data such as user name, display name, likes, tweets and retweets, replies, location, Twitter handle, following/followers, URL, date of creation, and more.

[Start Free Trial >](#)



a Twitter Image Scraper to
handle, following/followers,

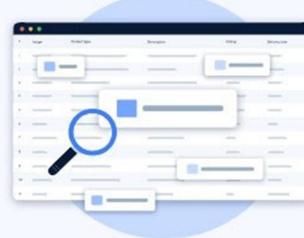
July 10, 2023

14 ||

Twitter Image Scraper

Scrape Twitter images and collect data such as user name, Twitter handle, following/followers, location, URL, date of creation, and more.

[Start Free Trial >](#)



Twitter Followers Scraper
of followers, profile URLs,

July 10, 2023

20 ||

Twitter Followers Scraper

Scrape Twitter followers and collect data such as: name, number of followers, profile URLs, images, company URL, and more.

[Start Free Trial >](#)



is proprietary technology
quickly and completely.”
[possible on the X platform](#)

26 [unless logged in as a registered user, the Twitter Profile Scraper required logged-in scraping or the](#)

27

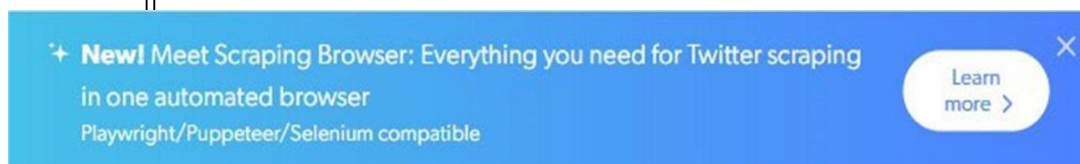
28

circumvention of X’s technological measures designed to prevent access to X data that is only available when logged in as a registered X user.

99. Defendant was and is aware that its scraping tools targeted at X’s platform may be used for logged-in scraping as well as public scraping.

100. 60.—In addition to these X-specific scraping tools, Bright Data offers an automated “Scraping Browser” that simplifies the act of scraping data from the X platform. As seen in Figure 14 below, Bright Data markets this product for scraping X Corp.’s data.

Figure 14: Screenshot of Bright Data’s website on July 10, 2023



101. 61.—Defendant advertises this “Scraping Browser” as containing “all website unlocking operations under the hood, including: CAPTCHA solving, browser fingerprinting, automatic retries, selecting headers, cookies, & Javascript rendering, and more.” Defendant also claims its Scraping Browser “automatically learns to bypass bot-detection systems as they adapt, saving you the hassle and cost.”

102. 62.—The Scraping Browser allows Defendant’s customers to “appear as a real user browser to bot-detection system[s],” such as those used by X Corp.

Bright Data Sells Proxy Services to Facilitate Data-Scraping

103. 63.—Defendant also facilitates the violation of X Corp.’s Terms by offering proxy services specifically designed to evade anti-scraping measures, including X Corp.’s CAPTCHAs and its registered user ID identification and IP rate limits. These tools allow unregistered users to impersonate actual registered X users in order to bypass X Corp.’s defenses digital fence and gates.

104. 64.—These proxy services imitate requests from legitimate users in order to conceal the true requestor’s IP address and location. Defendant advertises that these proxies will “avoid[] IP bans and CAPTCHAs” and allow users to “[g]ather vast amounts of public web data with total anonymity.” See Exh. J.

105. By posing as legitimate, registered X-users from repeatedly changing IP addresses using its proxy services, Bright Data accumulates guest pass tokens so it can use and sell them packaged with its scraping services at scale. This allows Bright Data and its customers to present “fake” guest pass tokens to pose as registered X users to pass through X’s technological gates.

106. Due to the “total anonymity” of the scraping which Bright Data thus enables, X users have no way of knowing which parties—whether Defendant or Defendant’s customers—have scraped their user and X’s content. Thus, any legal privacy restrictions which users must enforce themselves and to which Defendant or its customers is subject—whether provisions of the CCPA or the GDPR—is virtually meaningless: X users cannot enforce those privacy rights if they do not know whom to approach.

107. Consider that Bright Data ostensibly falls into the California Privacy Protection Agency’s classification of a “data broker” as a “business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship,” but Bright Data is not registered on the public California “data broker” registry as of May 31, 2024.⁸

108. Indeed, official governmental representatives from foreign countries such as Australia, Canada, the United Kingdom, Switzerland, Norway, New Zealand, Colombia, Morocco, Argentina, and Mexico recently issued a “Joint statement on data scraping and the protection of privacy” that highlighted the risks to privacy flowing from inadequate prevention of scraping by social media platforms such as X.⁹

109. Even if X users were aware of Bright Data’s scraping of their data, Bright Data does not in its Acceptable Use Policy provide analogous privacy features and control over X user data once Bright Data or its customers scrape it from the X platform:

⁸ Data Broker Registry, Cal. Privacy. Prot. Agency, https://cppa.ca.gov/data_broker_registry/ (last visited May 31, 2024).

⁹ Glob. Priv. Assembly, Int’l Enf’t Coop. Working Grp., *Joint Statement on Data Scraping and the Protection of Privacy* (Aug. 24, 2023), <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf>

- a. Bright Data does not require itself or its customers to delete or make private any data scraped from X after an X user has deleted or privatized it;
- b. Bright Data does not prohibit tracking of individuals based on the characteristics which X protects;
- c. Bright Data does not prohibit matching X usernames to users' legal identities or personally identifying information;
- d. Bright Data does not prohibit users from using geodata to track X users, including the creation of heat maps or user location profiles, even in circumstances in which that information is potentially highly sensitive;
- e. Bright Data does not prohibit its scraped data from being used (including by foreign governments) to assist in election interference, voter suppression, or the tracking and targeting of sensitive groups, including activists and political dissidents; and
- f. Bright Data does not prohibit its scraped data being used for individual profiling, psychographic segmentation, background and credit checks, or the development of facial recognition.

FIRST CAUSE OF ACTION

(Breach of Contract)

110. ~~65.~~ X Corp. realleges and incorporates all preceding paragraphs herein.
111. ~~66.~~ Use of the X platform and use of X Corp.'s services are governed by X Corp.'s

Terms.

112. ~~67.~~ X users, including Defendant, accept the Terms as a condition of using the platform.

113. ~~68.~~ Moreover, by virtue of having X accounts, Defendant has expressly accepted and agreed to X Corp.'s Terms.

114. ~~69.~~ The Terms are enforceable and binding on Defendant.

115. ~~70.~~ Defendant has repeatedly violated the Terms, including by (i) accessing the X platform through automated means without specific authorization from X Corp.; (ii) scraping data

1 from the X platform without authorization; (iii) selling tools that enable others, including X users, to
 2 access the X platform by automated means and to scrape data; (iv) selling proxy services that enable
 3 others, including X users, to access the X platform by automated means and evade X Corp.'s
 4 anti-automation and anti-scraping tools; and (v) selling data that Defendant scraped from the X
 5 platform.

6 116. ~~71.~~ Defendant has breached and continues to breach the Terms by scraping data from
 7 X Corp.'s platform without prior consent from X Corp. X Corp. has never authorized Defendant to
 8 access its platform through automated means and has never given Defendant consent to scrape data.

9 117. ~~72.~~ Despite being bound by the Terms, Defendant has repeatedly accessed the X
 10 Corp. platform through automated means and scraped data in violation of the Terms.

11 118. ~~73.~~ Defendant has breached, and continues to breach, X Corp.'s Terms by accessing
 12 the platform through unauthorized means and scraping data from the platform.

13 119. ~~74.~~ Defendant has breached, and continues to breach, X Corp.'s Terms by selling
 14 tools that allow other X users to access the platform by automated means and scrape data, and by
 15 selling proxy services that allow the same.

16 120. ~~75.~~ Defendant has breached, and continues to breach, X Corp.'s Terms by selling
 17 data that Defendant has scraped from X Corp.'s platform.

18 121. ~~76.~~ Defendant's conduct—both accessing X Corp.'s platform in volumes and
 19 manners that violate the Terms as well as selling data scraped from X Corp.'s platform—has
 20 damaged X Corp. and caused and continues to cause irreparable harm and injury to X Corp.

21 122. ~~77.~~ X Corp. is entitled to compensatory damages, injunctive relief, declaratory relief,
 22 and/or other equitable relief.

23 **SECOND CAUSE OF ACTION**

24 (Tortious Interference with Contract)

25 123. ~~78.~~ X Corp. realleges and incorporates all preceding paragraphs herein.

26 124. ~~79.~~ All X users must agree to abide by the Terms, which constitute a valid and
 27 enforceable agreement between X Corp. and each user.

1 125. ~~80.~~ As a user of X Corp.'s platform, as well as a present or former X account holder,
 2 Defendant is aware of the Terms and that they govern all users who choose to interact with the X
 3 platform. Defendant is also aware of the Terms because several of its executives and employees are
 4 present or former X account holders.

5 126. ~~81.~~ Nevertheless, Defendant has marketed and sold its scraping tools to X users and
 6 account holders, including X users and account holders residing in California, through its interactive
 7 website accessible in California and elsewhere, through its sales office and employees in California
 8 and elsewhere, and by using the X platform to market its scraping services to other X users and
 9 account holders.

10 127. ~~82.~~ Defendant has also sold proxy services and tools to facilitate automated access
 11 and scraping of the X platform by X users and account holders, including by locally offering a
 12 "Superior California Proxy" with "[v]ast numbers of California IPs to get data off any website."

13 128. ~~83.~~ By offering services and tools designed to provide automated access to the X
 14 platform, and to scrape data from the platform, Defendant induced a breach or disruption of the
 15 Terms by X users.

16 129. ~~84.~~ On information and belief, those who purchased Defendant's scraping services
 17 and tools used them to access X through unauthorized, automated means and to scrape data from the
 18 X platform, in violation of the Terms.

19 130. ~~85.~~ Defendant's conduct has damaged X Corp. and caused and continues to cause
 20 irreparable harm and injury to X Corp.

21 131. ~~86.~~ X Corp. is entitled to compensatory damages, injunctive relief, declaratory relief,
 22 and/or other equitable relief.

23 **THIRD CAUSE OF ACTION**

24 (Unjust Enrichment, in the alternative)

25 132. ~~87.~~ X Corp. realleges and incorporates all preceding paragraphs herein.

26 133. ~~88.~~ If Defendant's acts are found not to be in breach of contract, then Defendant's
 27 acts as alleged herein constitute unjust enrichment at X Corp.'s expense.
 28

1 134. ~~89.~~ Defendant used X Corp.'s service, platform, and computer network without
2 authorization to scrape data from the X platform.

3 135. ~~90.~~ Defendant receives benefits in the form of profits from its unauthorized scraping
4 of X Corp. data.

3 135. ~~90.~~ Defendant receives benefits in the form of profits from its unauthorized scraping
4 of X Corp. data.

5 136. ~~91.~~ Defendant's retention of the profits derived from its unauthorized scraping of
6 data would be unjust.

5 136. ~~91.~~ Defendant's retention of the profits derived from its unauthorized scraping of
6 data would be unjust.

7 137. ~~92.~~—Defendants’ conduct has damaged X Corp., including but not limited to
8 hampering the user experience for authentic X users and customers, in addition to the time and
9 money spent investigating and mitigating Defendants’ unlawful conduct.

7 137. ~~92.~~—Defendants’ conduct has damaged X Corp., including but not limited to
8 hampering the user experience for authentic X users and customers, in addition to the time and
9 money spent investigating and mitigating Defendants’ unlawful conduct.

138. ~~93.—~~X Corp. seeks actual damages from Defendants’ unlawful activities, an accounting, and disgorgement of Defendants’ profits in an amount to be determined at trial, compensatory damages, injunctive relief, declaratory relief, and/or other equitable relief.

138. ~~93.—~~X Corp. seeks actual damages from Defendants’ unlawful activities, an accounting, and disgorgement of Defendants’ profits in an amount to be determined at trial, compensatory damages, injunctive relief, declaratory relief, and/or other equitable relief.

138. ~~93.—~~X Corp. seeks actual damages from Defendants’ unlawful activities, an accounting, and disgorgement of Defendants’ profits in an amount to be determined at trial, compensatory damages, injunctive relief, declaratory relief, and/or other equitable relief.

13 FOURTH CAUSE OF ACTION

13 FOURTH CAUSE OF ACTION

13 FOURTH CAUSE OF ACTION

14 (Trespass to Chattels)

15 139. ~~94.~~ X realleges and incorporates all preceding paragraphs herein.

16 140. ~~95.~~ The X platform and all underlying technological infrastructure are the personal
17 property of X Corp.

16 140. ~~95.~~ The X platform and all underlying technological infrastructure are the personal
17 property of X Corp.

18 141. ~~96.~~ Defendant intentionally entered into, and made use of, X Corp.'s technological
19 infrastructure, including its software and servers located in California, to obtain information for its
20 own economic benefit.

18 141. ~~96.~~ Defendant intentionally entered into, and made use of, X Corp.'s technological
19 infrastructure, including its software and servers located in California, to obtain information for its
20 own economic benefit.

21 142. ~~97.~~ Defendant knowingly exceeded the permission granted by X Corp. to access its
22 personal property, including its technological infrastructure and servers.

21 142. ~~97.~~ Defendant knowingly exceeded the permission granted by X Corp. to access its
22 personal property, including its technological infrastructure and servers.

23 143. ~~98.~~ Defendant's acts have diminished the server capacity that X Corp. can devote to
24 its legitimate users, and thereby injured X Corp. by depriving it of the ability to use its personal
25 property.

23 143. ~~98.~~ Defendant's acts have diminished the server capacity that X Corp. can devote to
24 its legitimate users, and thereby injured X Corp. by depriving it of the ability to use its personal
25 property.

23 143. ~~98.~~ Defendant's acts have diminished the server capacity that X Corp. can devote to
24 its legitimate users, and thereby injured X Corp. by depriving it of the ability to use its personal
25 property.

25 property.

1 144. ~~99.~~ Through its acts, Defendant also caused other persons, including X users and
 2 account holders based in California and elsewhere, to knowingly exceed the permission granted by
 3 X Corp. to access its personal property, further injuring X Corp.

4 145. ~~100.~~ X Corp. has never consented to Defendant's conduct.

5 146. ~~101.~~ Defendant's conduct constitutes trespass to X Corp.'s chattels.

6 147. ~~102.~~ Defendant's acts have caused injury to X Corp. and if continued, expanded,
 7 and/or replicated unchecked by others, will cause damage in the form of impaired condition, quality,
 8 and value of its servers, technology infrastructure, services, and reputation.

9 **FIFTH CAUSE OF ACTION¹⁰**

10 (Unlawful, Unfair or Fraudulent Business Practices (Cal. Bus. & Prof. Code § 17200 et seq.))

11 148. ~~103.~~ X Corp. realleges and incorporates all preceding paragraphs herein.

12 149. ~~104.~~ Defendant's actions described above constitute unlawful, unfair, or fraudulent
 13 acts or practices in the conduct of a business, in violation of California's Business and Professions
 14 Code Section 17200, et seq, including because they constitute trespass and tortious interference with
 15 business relationships in violation of the law, and because Defendant deceived X Corp. into
 16 providing it access to, and information from, the X Corp. computer network. Defendant's data-
 17 collection technology and its data-scraping tools deliberately misrepresented the requests sent to the
 18 X platform, posing as legitimate X users, and Defendant's sale of IP proxies masquerades as a
 19 legitimate X user to avoid X Corp.'s technical measures designed to prevent unauthorized access of
 20 its computer servers.

21 150. ~~105.~~ Scraping data, as well as circumventing X Corp.'s ability to police its own
 22 platform, has caused substantial injury to X Corp., in the form of costs to investigate, remediate, and
 23 prevent Defendant's wrongful conduct, among other injuries.

24
 25
 26
 27 ¹⁰ Mindful of the Court's Order dismissing this claim, ECF No. 83, X Corp. includes the Fifth
 28 Cause of Action not for the purpose of re-argument but to preserve the issue.

(Misappropriation)

153. ~~108.~~ X Corp. has invested substantial time, labor, skill, and financial resources into operation and maintenance of X, its computer systems, and servers, including system and server security, as well as the ~~content on X~~aggregated data at scale. Defendant has not invested any of its time nor resources to the development of the X platform.

155. ~~110.~~ Defendant appropriated this aggregated data at scale at little or no cost to
 Plaintiff, free-riding on X Corp.'s substantial investment of time, effort and expense to aggregate
 data at scale.

156. ~~111.~~ As a result of Defendant's misappropriation, X Corp. has been forced to expend
 nal time, labor, skill and financial resources to investigate and mitigate Defendant's wrongful
 ct. Defendant has been able to exploit and profit from X Corp.'s substantial investments in
 platform and the creation of its aggregated data at scale.

157. ~~112.~~ X Corp. has been and will continue to be damaged as a result of Defendant's appropriation.

158. ~~113.~~ X Corp. has suffered and will continue to suffer irreparable injury, and its
law is not itself adequate to compensate it for injuries inflicted by Defendant.

WHEREFORE, Plaintiff prays for relief, as follows:

- 1 1. Preliminary and permanent injunctive relief enjoining Bright Data, its agents,
- 2 officers, employees and successors from:
- 3 a. accessing or using X Corp.'s website, servers, systems, and any data contained
- 4 therein for purposes of unlawful data scraping;
- 5 b. developing or distributing any technology or product that is used, or could be used,
- 6 for the unauthorized scraping of data from X;
- 7 c. facilitating the scraping of data by other users;
- 8 d. selling or offering for sale any data previously obtained from X;
- 9 e. utilizing any proxies to access X's website, servers, systems, and any data contained
- 10 therein; and
- 11 f. selling or offering for sale any proxies that can be used to access X's website,
- 12 servers, systems, and any data contained therein.
- 13 2. That Defendant be required to identify the location of any and all data obtained from
- 14 the X platform and to destroy any and all such data;
- 15 3. That Defendant be required to identify any and all recipients of data obtained from
- 16 the X platform;
- 17 4. Compensatory, statutory, and punitive damages, as permitted by law and in such
- 18 amounts to be proven at trial;
- 19 5. Reasonable costs, including reasonable attorneys' fees;
- 20 6. Pre- and post-judgment interest, as permitted by law;
- 21 An accounting of Defendant's profits from its scraping activities and disgorgement of those
- 22 profits; and
- 23 Any other remedy to which Plaintiff X Corp., Inc. may be justly entitled.

24 Dated: ~~November 14, 2023~~ June 6, 2024

Respectfully submitted,

HAYNES & BOONE LLP

By: /s/ Jason T. Lao

David H. Harper*

david.harper@haynesboone.com

Jason P. Bloom*

1 jason.bloom@haynesboone.com
2 2801 N. Harwood Street
3 Suite 2300
4 Dallas, Texas 75201
5 Telephone: (214) 651-5000
6 Telecopier: (214) 651-5940
7 *Admitted Pro Hac Vice

8 Jason T. Lao
9 jason.lao@haynesboone.com
10 Andrea Levenson
11 andrea.levenson@haynesboone.com
12 600 Anton Boulevard, Suite 700
13 Costa Mesa, California 92626
14 Telephone: (949) 202-3000
15 Facsimile: (949) 202-3001

16 *Attorneys for Plaintiff X Corp.*

17 /s/ Andrew H. Schapiro

18 QUINN EMANUEL URQUHART & SULLIVAN, LLP

19 Andrew H. Schapiro (Pro Hac Vice)
20 andrewschapiro@quinnemanuel.com
21 191 N. Wacker Drive, Suite 2700
22 Chicago, IL 60606-1881
23 Telephone: (312) 705-7400

24 David Eiseman (Bar No. 114758)
25 davideiseman@quinnemanuel.com
26 50 California Street, 22nd Floor
27 San Francisco, California 94111-4788
28 Telephone: 415-875-6600
29 Fax: 415-875-6700

30 Stefan Berthelsen (Pro Hac Vice)
31 stefanberthelsen@quinnemanuel.com
32 51 Madison Ave 22nd floor
33 New York, NY 10010
34 Telephone: (212) 849-7014

35 Attorneys for Plaintiff X Corp.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury of all triable issues.

Dated: ~~November 14, 2023~~ June 6, 2024

**QUINN EMANUEL URQUHART &
HAYNES & BOONE SULLIVAN, LLP**

By: /s/ ~~Jason T. Lao~~ Andrew H. Schapiro
~~Jason T. Lao~~ Andrew H. Schapiro